895

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/86494 A1

(51) International Patent Classification⁷: G06F 17/30, 17/60

(21) International Application Number: PCT/FI01/00430

(22) International Filing Date: 7 May 2001 (07.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20001074 8 May 2000 (08.05.2000) FI

(71) Applicant *(for all designated States except US)*: SONERA OYJ [FI/FI]; Teollisuuskatu 15, FIN-00510 Helsinki (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: MÄKELÄ, Teemu [FI/FI]; Jämeräntaival 6 c 221, FIN-02150 Espoo (FI).

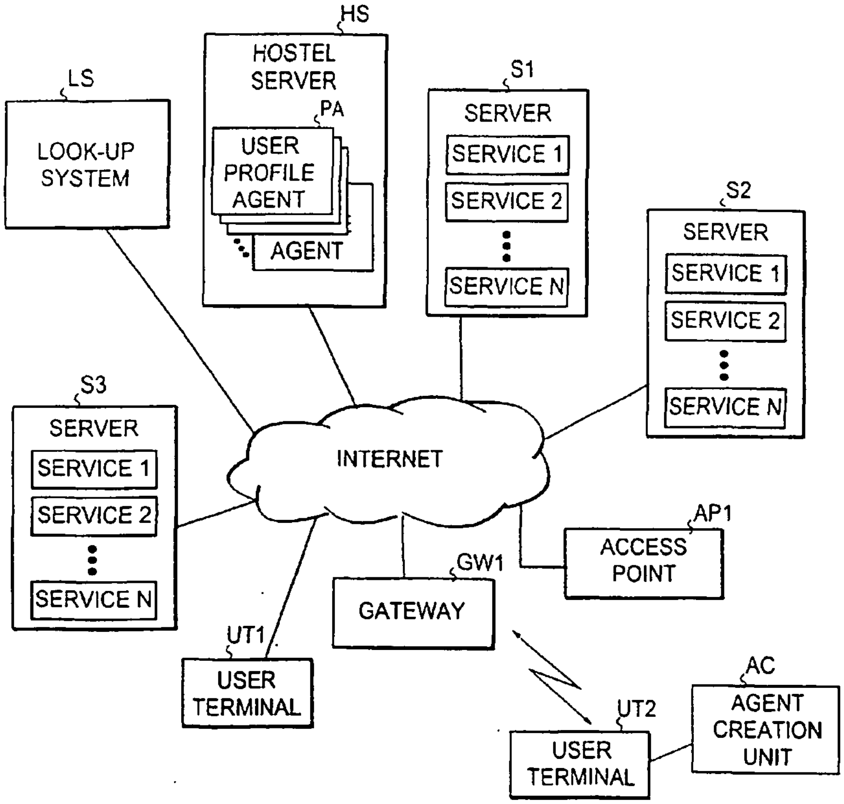
(74) Agent: PATENT AGENCY COMPATENT LTD.; Pitkänsillanranta 3 B, FIN-00530 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: USER PROFILE MANAGEMENT IN A COMMUNICATIONS NETWORK



(57) Abstract: The invention relates to a system for providing user-specific information in a communications network. User profile data is stored in user-specific software agents, each agent comprising at least an inner layer for storing the user profile data and an outer layer for storing contracts. The contracts are used by the service applications residing in the network for obtaining user-specific information from the agents. An individual contract determines the items that the service application associated with that contract sees from the user-specific data and also how the service application can process said items. The current locations of the contracts are maintained in a separate location information system so that the location of a desired contract can be requested from the said system before user-specific information is transferred between a service application and an agent.

Published:
— *with international search report*

USER PROFILE MANAGEMENT IN A COMMUNICATIONS NETWORK

Field of the Invention

The invention relates generally to provision of services in a communications network. More specifically, the invention relates to a system for providing user-specific information in a network where personalized services are provided.

Background of the Invention

The strong growth in the number of Internet users and services provided through the Internet has been one of the most remarkable phenomena in communications in recent years. The popularity of the Internet shows that people are eager to adapt technology to their lives. However, as the spectrum of services available on the Internet and their complexity increase, the task of gaining maximum value from the services becomes increasingly complicated. As a simple example, if a currently available Web search engine is given a simple query, thousands of pages of irrelevant material is normally obtained, which has to be browsed through manually. Another example can be taken from the telecommunications world. In the emerging open telecom market, the users will have the opportunity to buy affordable services matching their requirements and preferences. This may involve complicated decisions concerning the features of the customized services and the selection of the service provider, especially when the customer roams outside his/her home network. In order to maximize the gained utility, users have to get to know multiple providers, and enter into negotiations with them. Too often this is an insurmountable task; users are overwhelmed with more alternatives or more information than they can easily handle. This growing complexity is partly due to the transformation of the traditional search engines into Web portals offering a broad array of services.

In both of the above-mentioned cases, semi-intelligent techniques could be employed to automate the selection process. However, in order to achieve the desired goals, something has to be known about the user. This knowledge makes up the user profile. What the profile contains, depends on the particular service, but the ultimate goal could be seen as forming a metauser, a high-level description of the user. Service providers can then utilize this description in order to offer services adapted to each user. In other words, by means of these profiles the service providers can adapt the applications' behaviour to the users. The process of generating the user profiles, or learning to know the users, is called profiling.

Profiling has become an important issue in solving the above problems related to complex services and overwhelming information flow. This is because profiling enables personalization of the services, which in turn provides customized aids to help individual users to cope with the above problems. Personalization is the process of applying the knowledge in the user profile in order to provide results fitting the needs of a particular user. Today, many Web portals are moving in this direction by providing means for filtering the information content based on the interests of the user.

Although personalization is seen as a solution in overcoming the above problems, present technology is still immature, and there are many problems related to the existing systems. These are discussed briefly in the following.

At present, users have to supply their profile data to each individual service provider. Therefore, a lot of resources are needed to create accurate profiles not only by the service providers, but also by the users. Beginning from the registration for a service, the users fill out numerous forms about their personal characteristics, and increasingly also about their preferences. From the initial information and observations during interaction with users, the services then form profiles of the users. Teaching every new service provider from scratch takes time and becomes a frustrating task for the user. Since the user has to input profile information for each service provider, the information relating to a single user scatters all over the network, and different service providers have different kinds of information about the user. One drawback of this is that one profile cannot be used, at least not directly, by another service provider. The management of the profiles also becomes a problem. For example updating an email address for every service easily becomes an insurmountable task. Even if the facilities were provided by the services, recalling each of those who should be notified is hard. Thus, the users' capabilities and motivation to maintain the profiles are poor, and the accuracy of the profiles is reduced.

A further problem related to having each service maintain its own profile on each user is that an individual service's view of the users is very limited. Therefore, the user cannot benefit from the service in the most efficient way.

Another major problem relating to the present situation is the privacy of the users. It is clear that the storage of personal data, such as the user profiles, in an open and shared system like the Internet requires careful consideration of user privacy. Since the users are, in the current situation, unable to comprehensively control the contents and the use of their profiles, the privacy of the users can easily be invaded. For example, an individual user has no means to prevent a malicious party from accessing the profile data on a single server or from combining the data on different servers.

Some currently implemented systems that employ a user model operate locally in the user terminal (e.g. a personal computer). One example of this kind of system is depicted in U.S. Patent 5,913,030, which describes a system for communications between a client system and a server communicatively coupled to the client system. Information about a user is stored in the client system (i.e. in the client terminal). The user information comprises a plurality of attributes, each attribute comprising information relating to the user and a willingness indicator indicating the level of willingness of the user to reveal information concerning that attribute. The terminal can also include several persona modules, each containing data defining a particular persona of the user. The privacy of the user can further be protected by sending user-specific data to a trusted third party which reveals only aggregate demographic information about all the users to the server providing the service. The persona module can also be provided with a disguising function which generates incorrect information about the user.

The main drawback of the systems where the user profile resides in the user terminal is that the utilisation of the user model is restricted to that terminal, i.e. typically to a fixed place, and the dissemination of the items of the user model is restricted.

Currently, there are also server-based systems which allow a user to use personalized Web services while providing privacy. One such service is ProxyMate (former Lucent Personalized Web Assistant, at www.proxymate.com). ProxyMate focuses on offering users the means to interact with multiple servers so that an individual server providing a specific service can not reverse-engineer the identity of the user, but at the same time the user can be recognized and authenticated on repeated visits. This is achieved via generation of secure, consistent and pseudonymous aliases for Web users, and by anonymizing traffic to the Web servers. ProxyMate also acts as a mediator for e-mail.

An important design criterion behind ProxyMate has been statelessness. It does not keep any long-term states, i.e. mappings between users and their aliases. Instead, all the aliases are generated on demand via a one-way function.

ProxyMate works as a proxy for Web traffic. Hence, it can be located and used from anywhere in the network. These server-based systems require trust from their users. Although their theoretical construction is such that they do not require any state to be maintained outside the session, the implementation might, for example, collect a log of the user's actions. A further drawback of these served-based systems is that the user's connection to the server providing the service always goes through these proxy servers. This restricts the ways the desired data can be accessed. Further, constant routing through certain proxies results in inefficient use of the transmission resources of the network, and these proxies may become bottlenecks having an adverse effect on the response times of the services.

It is an object of the invention to obtain a solution by means of which it is possible to alleviate or eliminate the drawbacks described above and to bring about a system which provides the users of the network with full and comprehensive control of their profiles.

Summary of the Invention

This and other objectives of the invention are accomplished in accordance with the principles of the present invention by providing a system in which the profile data relating to a single user is placed with a profile agent dedicated for the use of that user only. Thus, each user is provided with a profile agent by means of which he/she can control his/her digital identities, i.e. the identities that the service applications see as the user. In this way it is possible to provide, by means of a single profile agent, applicable profile information to a large number of services needing different kinds of profile information.

Each user-specific profile agent has a multi-layer structure so that the user profile data can be accessed only through the uppermost layer comprising contracts which form the interfaces between the user-specific data and the network. The user-specific profile agents are accommodated in special servers, which are in this context termed hostels, and the network further comprises a lookup system from where the location of a certain contract can be queried. The service applications can access the user-specific data only through the contract after such a contract is made for this purpose. The contract determines the information items that the service application sees from the user-specific data and also how the service can process said items. Each contract forms an interface of the user-specific data for a service or group of services. The contracts thus associate certain views or profiles with certain services. However, one service can also use more than one contract to access the user-specific data. In this case the service cannot recognize that the two contracts relate to the same user.

In a preferred embodiment of the invention the user profile data are disseminated only via user-defined digital identities. These identities form a layer between the contracts, which form the outermost layer of a user profile agent, and the basic profile data, which form the innermost layer of a user profile agent. The basic data can not be accessed by any service. The identities, which are also called personae in this context, represent consistent views on the basic profile data of the user. The services see these views only, and they are unable to distinguish whether two different views belong to the same user or not.

The privacy of the users thus has a central position in the system, since the user profile is centralized with an agent which can be controlled by the user, or by a party authorized by the user. Further, it is difficult to determine that two contracts are related and to expose the agent behind the contracts.

Furthermore, as the profile agents can be mobile, they are no longer bound to certain providers, and the lifetime of the profiles becomes unlimited.

Brief Description of the Drawings

In the following, the invention and its preferred embodiments are described more closely referring to the examples shown in Figures 1 to 14 in the appended drawings, wherein:

Figure 1 illustrates the architecture of the system according to the present invention,

Figure 2 illustrates the general structure of an individual user-specific profile agent,

Figure 3 illustrates the cooperation of a service application with the profile agent,

Figure 4a illustrates a typical structure and information content of the lowermost layer of the user profile agent,

Figure 4b illustrates a typical structure and content of an individual item inside the lowermost layer of the user profile agent, Figure 5 illustrates an example of the contents of the lowermost layer of a user profile agent,

Figure 6 and 7 are examples of the contents of two different personae on the middle layer of a user profile agent,

Figures 8 and 9 are examples of the contents of two different contracts on the outermost layer of a user profile agent,

Figure 10 illustrates an example of message transfer between the elements of the system when the user creates a profile agent for herself/himself,

Figure 11 illustrates an example of message transfer between the elements of the system when a contract is created for a service application,

Figure 12 illustrates an example of message transfer between the elements of the system in conjunction with a general information request received by a user profile agent,

Figure 13 illustrates an example of message transfer between the elements of the system when the user profile agent moves in the network, and

Figure 14 depicts the structure of the lookup system.

Detailed Description of the Invention

Figure 1 shows the architecture of the general system according to the present invention. The system includes several servers (S1 to S3) which offer a broad array of resources and services for the users of the network. In this example, all the servers are nodes of the Internet or an Intranet network (or an equivalent TCP/IP network). In this context the term "service" refers to a service application residing in a server.

User terminals (UT1 and UT2) have access to the service providing servers in a manner known as such. The user terminals can be fixed terminals, as shown in conjunction with terminal UT1, or mobile terminals that have wireless access to the system or to the network, as shown in conjunction with terminal UT2. Wireless access can be implemented through various access points (AP1) or alternatively through gateways (GW1) that translate the requests from the protocol stack used between the terminal and the gateway, such as the WAP protocol stack, to the protocol stack used between the gateway and the server, i.e. to the WWW protocol stack (HTTP and TCP/IP).

In terms of the inventive idea, the types of the user terminals and the connections between the user terminals and the service providing servers are not of significance. In this context the only essential feature of the terminals is that they are provided with browsers or other known client software by means of which they can communicate with the servers providing services. This communication occurs preferably according to HTTP protocol, although there can be a translating gateway between a server and a client terminal, as mentioned above.

The system further comprises user-specific profile agents PA so that each user of the system preferably has one profile agent assigned to that user only. A profile agent here refers to a piece of software that can accomplish tasks on behalf of its user and which stores the profile data related to the user. Thus, an individual profile agent is an integral entity to which the user can delegate the task of coordinating his/her profile. The structure of an individual profile agent, consisting of code and data, is discussed below in connection with Figures 2 and 3. The agents are implemented using known agent technology.

The profile agents are located in specific servers, called hostels in this context. A hostel is simply a platform (i.e. a piece of software) that offers an execution environment for the profile agents and a connection to the network. For simplicity, Figure 1 shows only one hostel HS, although there are typically many hostels in the network.

The system further includes agent creation units AC, by means of which the users can create their profile agents. Agent creation units can reside in the user terminals or in conjunction with the hostels, for example.

Each user-specific profile agent is controlled only by the user in question. Thus, in the system according to the present invention the user profile is centralized with an agent controlled by the user. A user-specific profile agent can be in a fixed location or it can be a mobile agent, especially if the user is mobile. A mobile profile agent preferably moves so that it is always in the hostel nearest to the current location of the user.

To promote profile agent mobility the system further includes a lookup system LS which stores the current location of each individual profile agent and from which the locations of the profile agents can be queried. The structure of the lookup system is discussed in more detail below, where it is depicted that the location of each profile agent is stored as a plurality of locations, each location indicating the current address of the individual contract which is part of the profile agent.

Figure 2 depicts the structure of an individual profile agent from the point of view of its clients. The agent preferably has a three-layer structure with the user base profile forming the lowermost layer. The base profile typically includes all data about the user, said data being supplied by the user or the clients. The middle layer includes the different digital personae of the user. Each persona is formed from the data in the base profile and it is a certain view of the base profile, the view being defined by the user. An individual persona or view can be formed passively, i.e. it can consist of data units that form a subgroup of the data units in the core profile, or actively, i.e. the desired data units in the base profile can be processed to obtain the data units forming the persona.

The topmost layer of the profile agent consists of interfaces which are here called contracts. Contracts are the interfaces through which the user and the services can access the profile agent. The user always accesses the profile agent through a special contract, called master contract, which is for the use of the user only. The service applications access the digital personae through service contracts, i.e. the services can only point to the contracts, not to the personae behind the contracts. To be able to access the profile data, each service must first make a contract with the profile agent. After a contract is made, the service can utilize the profile agent through the said contract (interface). Each agent typically includes one contract per service provider or service application, although one contract can be for a group of applications/providers and one service application/provider can also use several contracts.

Thus, the identity of the user is controlled by the contracts. While from the standpoint of the architecture the contracts mainly represent pseudonymous contact points to the profile data, to the users their most important function is to set the limits to the information that is available to the clients (i.e. to the services). The profile agent needs to allow transformation of the base profile items from views to a base profile, and vice versa. The transformations usually needed are quite simple, such as replacing a name with an alias and emphasizing different interest areas of the user. A transformation from the base profile is made for a certain context. Generally, transformation is made for all valuations of the dimensions – who, where, when and what. These dimensions could be modeled as independent, so that the transformation could be the sum of transformations for all dimensions. In effect, the user could be represented by a base profile, and sets of transformations for each dimension. By selecting a suitable set for each dimension, and layering these upon the base profile, strong expressiveness with respect to the context can be achieved.

Figure 3 illustrates the cooperation of a profile agent with a service application. Each contract CT on the uppermost layer handles access rights controlling both the entities who can access the profile agent and what those entities are allowed to do if access is allowed. The personae of the user, in turn, corresponds to the views of the user available to the service applications. The views are formed from the base profile of the user, either directly or through transformations.

Maintaining a broad spectrum of transformation sets is outside the user's capabilities. On the other extreme, total lack of transformations is not to be preferred either. Thus, the user profile agent is preferably based on a compromise of these two, i.e. the user fixes the transformation to some context. In effect, the transformation defines a persona of the user – e.g. a home or business persona. Furthermore, the personae are separated into their own layer, so that they can be used in multiple contracts and so that one contract can allow the use of multiple personae.

The base profile contains the user's whole profile organized in a hierarchical manner. Figure 4a illustrates an example of a base profile organized in different categories by the content of the profile. In this example, the first category includes the unique identifiers of the user, the second category biographic and demographic data about the user, the third category the addresses of the user, the fourth category data about the interests and attitudes of the user, etc., and the last category data about the current location and activity of the user.

Each category in the base profile includes a plurality of items. Figure 4b illustrates an example of the structure of an individual item. The content of an item is divided into data units describing the item. In the example of Figure 4b, the first data unit represents the name of the item, the second gives a description of the item, the third indicates the type of the item, the fourth describes how the item is transformed for a persona of the user, and the last one includes the value of the item. By making the items separately addressable, the user can control the access to individual items. As is obvious, the number and type of items in an individual category can vary, depending on the category and on the user, for example. The number of hierarchy levels in the base profile can also vary.

Figure 5 illustrates an example of the contents of one base profile forming the lowermost layer of an agent. In the figure, the categories or items at the same hierarchy level have been indicated with bullets that are white at every other level and black at every other level. In this example, the user is Joe Doe, whose nickname is "Foobar". In the base profile, the "transformation" field describes all the transformations that are possible for that item. For example, the gender of the user can be switched between male (M), female (F), and neutral (N). In the model/preferences category, different service providers can gather information about the user preferences. In this example, the said category includes relative values indicating how frequently the user uses the sports, business, and weather services provided by the service portal at www.company1.com. If a certain agreed ontology is used for user preferences, all service providers can utilize this information for their purposes.

In practice, the base profile normally includes much more information than in the example of Figure 5, which only illustrates what kind of data the base profile can include.

Figures 6 and 7 show two examples of the personae of the user whose base profile is shown in Figure 5. Figure 6 illustrates a business persona which can be used during office hours, for example. In this persona, the above-mentioned business channel at www.company1.com gets more weight than the other services, i.e. this persona is more interested in the business channel than in the other services. Moreover, the nickname of the user is masked from the services, i.e. the services do not see the nickname of the user. Figure 7 illustrates a second persona, here called an online persona, which can be used in sessions initiated from home, for example. For this persona, the gender of the user is changed to neutral, the income value is rounded to the nearest 10000, all the items in the name category, except the nickname, and also all the items under the home address are hidden.

Figures 8 and 9 illustrate the contents of the contracts on the outermost layer of the user profile agent. Figure 8 shows a master contract which is used by the user only. To enable secure communication with the user, the master contract stores the public key of the client (PKU01) and public and secret keys of its own (PKM01 and SKM01). The client of the master contract is always the user whose master contract is in question. Figure 9 shows an example of a general contract for a service which is here marked as "service01". Through this contract, two services can access the user profile data, i.e. services with the public keys PKS01 and PKS02. The contract can define the items of the base profile that can be accessed through the contract (cf. access rights/type=allow). In this example, the items in the model/preferences category can be read and written, whereas the items in the identifiers category and under properties/income can only be read. The contract can also define the items of the base profile that are not allowed to access through the contract. In this example, the postal address categories can not be accessed at all (access rights/type=deny).

The contract can further determine the personae (views) that can be seen through this contract. In this example, only the online persona can be seen through the contract. Thus, even if the user is currently using the business persona, service01 would see the online persona. The contract can also determine different policies for different services. The contract of Figure 9 includes one policy: if the recipient, i.e. the service provider, is "company01", indicating that the items are for its use only, all the items can be accessed which are not masked or otherwise hidden. As discussed below, the user controls what items can be seen through the contract, and in which form the items can be seen. In the contracts, the standard format according to P3P (the Platform for Privacy Preferences Projects) can be used to inform the service provider of the privacy practices adopted by the profile agent (i.e. the user).

In this way the contract further defines the views on the middle layer of the agent. The agent can also include several middle layers, each manipulating the view on the preceding layer. Determination of the data available to a client is preferably done so that the definition of the set of data available to a client gets more accurate and detailed moving from the base profile towards the outermost layer of the agent.

Each user profile agent is preferably created by the user in question. Figure 10 illustrates an example of message transfer between the elements of the system when the user creates a profile agent for himself/herself. For the creation of an agent the system according to the present invention includes the above-mentioned agent creation units. Each agent creation unit is a piece of software that allows the user to create a user profile agent. The agent creation units can reside in the user terminals, in conjunction with the hostels, or in separate Web sites offering this service for the users. The messages exchanged are preferably always encrypted when the public key of the opposite party is available.

Initially, the user terminal sends the agent creation unit a message requesting the said unit to initiate the creation of a user profile agent (step 1001). This message includes the public key (P_KEY_U) of the user. In response to this message, the agent creation unit generates an empty profile agent for the user. When this has been accomplished, the agent creation unit requests the profile agent to create a master contract to allow the user to manipulate the agent through the said contract (step 1003). This request also includes the public key of the user. The user profile agent then generates an identifier (CID) for the master contract (step 1004) and a key pair for the master contract. The master contract now has the keys shown in Figure 8 for encrypted communication with the user. The user profile agent then informs the agent creation unit about the new contract by sending the creation unit an export message including the identifier and the public key (P_KEY_MC) of the newly created contract (step 1006). In response to this message the agent creation unit sends the lookup system a registration request (step 1007). This request includes the identifier and the public key of the master contract as well as routing information pointing to the location of the profile agent. However, the routing information in this example is null (empty), since the user profile agent has not yet been moved to its correct location in the network. Upon receiving this message, the lookup system checks that the identifier is not being used by any existing contract. If the identifier is not in use, the lookup system registers the contract and sends an acknowledgment to the agent creation unit (step 1008).

After this the user profile agent is moved to its correct location, i.e. to a hostel (step 1009). If the agent creation unit and the profile agent are already in a hostel, this step is naturally omitted. The migration of the agent typically includes several messages, although only one is shown in the figure.

After migration, the identifier of the contract is re-exported to the lookup system with proper routing information pointing to the hostel (step 1010). This is performed so that the hostel first activates the agent. As a result of this, the agent asks the hostel to perform the re-export, and the hostel sends the message to the lookup system. The agent creation unit then acknowledges the creation of the master contract to the user at step 1011. This acknowledgment message includes the identifier and the public key of the master contract. The user profile agent is now fully usable, although it is still empty.

The user then has to supply data to the user profile agent. For this purpose, the user terminal first requests the routing information of the profile agent from the lookup system by sending a request including the identifier of the master contract (step 1012). Having received the routing information pointing to the hostel in which the user profile agent resides, an update message is sent to the hostel at step 1014. This message includes the identifier of the master contract, the operations to be performed, and the data to be used by the operations. The hostel forwards the message to the profile agent. For example, if the user has created a base profile according to Figure 5, the message would contain the following write operations and data:

update("Identifiers/name/first", "John")
update("Identifiers/name/middle", "Bar")
update("Identifiers/name/last", "Doe")
update("Identifiers/name/nickname", "Foobar"), etc.

Thus, the user sets the desired data in the profile agent through the master contract whose address is first retrieved from the lookup system. This may require that several update messages are sent to the hostel.

After the profile agent has performed the desired operations, it acknowledges the operations (step 1017) to the hostel, which forwards the acknowledgment to the user terminal (step 1018).

The user profile agent is now ready for the service applications. If the user later wants to update his/her existing profile agent, the update occurs as in steps 1012 to 1018 in Figure 10, i.e. routing information pointing to the correct hostel is first requested from the lookup system, and then one or more update messages are sent to the hostel where the profile agent resides.

When the user contacts a service that wants to utilize the profile data, a contract must first be made for the service. Figure 11 illustrates an example of message transfer between the elements of the system when a new contract is created between the user profile agent and the client (i.e. the service provider/application). First, the user sends a conventional service request to a Web site (step 1101) providing services. In response to the service request the user typically receives a registration page from the server (step 1102). After this, the user has to access his/her profile agent. For this purpose, he/she then sends the lookup system an import message requesting the address of the master contract from the lookup system (step 1103). In response to the message, the lookup system returns routing information to the user, the routing information indicating the current location of the master contract. In this example it is assumed that the user profile agent is currently in hostel A.

The user then sends a message to hostel A (step 1105), requesting a generation of a contract for the service. This message includes at least the identifier of the master contract as well as the public key of the service (P_KEY_S) which has been received earlier in connection with the registration page. The hostel finds the user profile agent corresponding to the master contract ID received and forwards the message to the said profile agent at step 1106. In response to the message, the user profile agent then generates a contract ID and a key pair for the service (step 1107), and the agent exports the generated contract ID (CID) and its public key (P_KEY_C) to the hostel (step 1108). The hostel knows what node of the lookup system is available and sends a request to this node at step 1109. This request asks the lookup system to register the new contract. The message includes the ID of the contract, the public key of the contract, and routing information pointing to hostel A. The routing information given in this message indicates a different route to hostel A as compared to the route given at step 1104, so that the master contract and the service contract cannot be linked together by means of their location.

If the registration of the new contract was successful, the lookup system acknowledges the operation to the hostel (step 1110), which further acknowledges it to the user profile agent (step 1111).

After this, the user is informed of the ID of the newly generated contract. The user profile agent first sends the ID and the public key of the contract to the hostel, which forwards the message to the user terminal (steps 1112 and 1113).

When receiving this information, the user terminal updates the contract according to his/her preferences at step 1114. In other words, at this step the user determines the views that can be seen through this contract by defining at least the outermost layer of the profile agent. This step determines what items the service provider/application can see, and in which form, and what the service provider is allowed to do with the contract.

After this, the user terminal sends the server providing the service a reply to the registration page received at step 1102. This message at step 1115 can be a normal HTTP-POST message including the contract ID and the public key of the contract.

As described above, in this basic scenario the user initiates the relationship between the service and the user profile agent by sending the identifier of the new contract to the server providing the service. In response to this message, the server requests routing information to the hostel of the agent from the lookup system (step 1116). When the server receives this information at step 1117, it knows that a contract exists, i.e. that the user is not trying to bluff. The server then requests information from the user profile agent by sending an information request to the hostel, which forwards the request to the profile agent (steps 1118 and 1119). The request includes the ID of the contract, the operations, and the arguments relating to the operations. For example, if the server asks for the data that is under the sub-category "name" in the user profile, the operation is "read" and the arguments include "identifiers/name".

The user profile agent first authenticates the request and then processes it. In response, the required information is returned to the server (steps 1121 and 1122). If a contract according to Figure 9 was created earlier, the user profile agent notices at step 1120 that the online persona must be used. Since the online persona is such that under the sub-category "Identifiers/name" only the nickname can be shown, the user profile agent returns only the nickname (Foobar) at step 1121. When the server receives this message, it can continue its normal operation by welcoming the user to the Web site (step 1123). This HTTP response then includes the nickname of the user in the body of the message. After this, the user can use the service.

If the service wants additional information about the user later in connection with the same or a subsequent service session, the service sends a request for information to the user profile agent. Figure 12 illustrates an example of message transfer between the elements of the system in conjunction with such a general information request coming from the server providing the service. The server again first requests routing information to the hostel of the profile agent from the lookup system and upon receiving it sends the information request to the hostel (steps 1201 to 1203), which forwards the request to the user profile agent (step 1204). In this connection, it is possible to define that if the operation requested by the service is such that it is not allowed, permission is requested from the user terminal. The user profile agent then asks for permission from the user terminal by sending a verification request to the user terminal via the hostel (step 1205). If the user allows the operation, it returns an acceptance (step 1206). When the user profile agent receives this message, it starts to process the request and then sends the desired information to the service (steps 1207 and 1208). For example, if the requested operation was "write", the user profile agent returns the status of the request (i.e. request accomplished). Should the user terminal deny the operation required by the service, the service is informed that the operation requested is non-allowable. On the other hand, if no verification of the operation is required, the user profile agent replies the service directly after the request.

As mentioned above, the user profile agent can also move in the network. For example, if the current location of the user has been updated by an entity, such as a GPS receiver, the user profile agent can notice that it is too far away from the current location of the user. The user profile agent then initiates a location update by sending the current hostel a migration request, see Figure 13, step 1301. This message can include the address of the new hostel located near the current location of the user terminal, or, if the user profile agent does not know the nearest hostel, the message includes the current location of the user together with a request to move the agent to the hostel nearest to said location. As a result, the new hostel (hostel B) is sent a request to accept the user profile agent (step 1302). If the new hostel accepts the profile agent, it sends an acknowledgment to the current hostel (step 1303). Upon receiving this message, the current hostel asks the user profile agent to serialize itself (step 1304). In response to this, the agent is transferred in serialized format to the new hostel (steps 1305 and 1306). This new hostel then activates the user profile agent at step 1307. In response to the activation, the user profile agent sends the new hostel a location update request for each of the contracts, one contract at a time. Figure 13 illustrates the location update of two contracts (CID_1 and CID_2, steps 1308 and 1312, respectively). The messages sent by the user profile agent include the identifier and the public key of the contract. In response to each request from the user profile agent, the new hostel sends the lookup system an update request inserting routing information into the message (steps 1309 and 1313 for the first and second contract, respectively). The lookup system updates the location of the contract indicated in the request and sends an acknowledgment back the to the hostel (steps 1310 and 1314), which forwards the acknowledgment to the user profile agent (steps 1311 and 1315). When the user profile agent has received an acknowledgment from each update process, it sends the new hostel an acknowledgment request (step 1316). In response to this message, the new hostel acknowledges the transfer of the agent to the original hostel (step 1317).

In this way the new hostel updates the location of the user profile agent contract by contract. The locations are updated one contract at a time in order to prevent the lookup system from detecting that the contracts belong to the same user profile agent.

The lookup system operates like a black box in serving the rest of the system. The contact points (i.e. the contracts) are registered there, via a location update operation, and are requested from there, via a lookup operation. Additional requirements for the lookup system are that it should be efficient and scalable. Thus, the capabilities of the lookup system should not hinder the mobility of the user profile agents. The options for implementing the lookup system are discussed briefly in the following.

As the profile agent knows its clients, the simplest choice would be for the profile agent to keep the clients aware of its whereabouts. However, through collaboration the clients could observe when each pseudonym (persona) changes its location, and thus could correlate which pseudonyms are likely to be linked to the same person. In particular, this would prevent the users from having two contracts with a client.

Utilizing forwarding chains is another option for the implementation of the lookup system. In this solution the agent leaves a forwarding address at its previous hostel when it migrates to a new hostel. By following the resulting chain of forwarding addresses, a client can then find the agent. The drawback of this approach is that it performs poorly in situations where the agents are highly mobile – the length of the chain grows, and the search path might bounce from one side of the globe to the other.

The home-based approach eliminates the erratic search paths in the forwarding chain approach. In the home-based approach, each user profile agent would have a designated server – home – to keep track of its location. However, this approach limits mobility, binding the user to its home provider.

The name server approach is a traditional way to link identifiers to their locations. It is employed, for example in the Internet's Domain Name System. Name server systems are highly scalable, as the parts of the identifier space are distributed hierarchically over different servers. Unfortunately, hierarchical addressing assumes that address binding is relatively stable.

To maximize personal mobility, the addressing must be flat, and the name server approach is not possible. A location service that is based on a flat address space is described in an article by Ballintijn, van Steen, and Tanenbaum: Exploiting Location Awareness for Scalable Location-Independent Object Ids, Proceedings of Fifth Annual ASCI Conference, Heijen, Netherlands, June, 1999, pp. 321-332 (also available at http://www.cs.vu.nl/pub/papers/globe/IR-459.99.pdf, visited 4/2000). The lookup system according to the present invention is preferably according to the system described in this article. A central notion in this location service is the exploitation of locality, meaning that the cost of a lookup increases with the distance to that address – i.e. it is cheaper to find local objects.

The structure of such a lookup system is illustrated in Figure 14. The basic architecture is hierarchical so that the nodes of the system divide the network into a hierarchy of geographical domains. At the bottom of the hierarchy are the leaf nodes, each leaf node covering a leaf domain which may in practice cover an area of a few LANs. The next higher level domain may then represent the city where the LANs are, for example. Associated with every domain is a directory node, which stores location information for the contracts within its domain (i.e. the domain covered by the nodes below it). The root node at the top of the hierarchy covers the whole network and contains pointers for each identifier to the node in the next level, and so on. The leaf nodes store the addresses of the contracts. Thus, only one leaf node knows in which hostel the contract resides. When a lookup takes place, the lookup operation is started from the leaf node corresponding to the domain where the client is. If the leaf node has the address, the client gets the address immediately. Otherwise the request is propagated upwards until it reaches a directory node containing a record of the searched identifier, from where it propagates downwards to the leaf node where the address is.

As the structure and operation of the lookup system is known as such, it is not discussed in more detail in this context. More information can be found from the above-described article or from an article by M. van Steen and F. Hauck: Algorithmic Design of the Globe Wide-Area Location Service, The Computer Journal, 1998, Vol. 41, No. 5, pp. 297-310 (also available at http://www.cs.vu.nl/pub/papers/globe/IR-459.99.pdf).

Although the invention was described above with reference to the examples shown in the appended drawings, it is obvious that the invention is not limited to these, but it may be modified by those skilled in the art without departing from the scope and spirit of the invention. The following describes briefly some possible variations.

The system can support three different communication modes with the profile agents: stateless, session-based, and event-based modes.

In the above-described stateless communication mode no long-term information about the location of the profile agent is kept outside the lookup system. This mode enables a simple request-response message exchange. Since the other modes pose security risks, stateless communication is the preferred way of communication for the majority of the clients. For each message exchange, the clients first lookup the location of the profile agent and then perform the message exchange, including the authentication.

A session-based communication mode enables the clients to commence a long-term relation with the profile agent. Should the profile agent migrate during this period, the session is also migrated. Furthermore, authentication and policy notification are performed only once. However, when the profile agent sends notification of the new address to the clients, they can engage in a correlation attack based on the arrival time of the updates. Thus, the use of session based communication should be limited to trusted clients only.

Event-based communication can be used for distributing changes in the profile. In this mode the clients subscribe to receive notification of certain items. When the profile agent receives an update on an item, it sends notification to all subscribers of that item.

Events can also be utilized in correlation attacks. However, the potential can be reduced by making their delivery more asynchronous, e.g. by inserting varying delays between each notification to be sent.

The user profile agent can also be a distributed object comprising a mother agent and several child agents. Thus, different contracts can reside in different hostels. The benefit of this implementation would be that the user no longer has to trust a single hostel with all information, except for the hostel of the mother agent, which can still access all parts of the profile but no longer knows all the clients with whom the profile agent has a relationship.

The profile agents can also be implemented without storing the views for subsequent information requests. In this case a view is formed by the profile agent each time profile information is requested, using one or more functions determining the view. In this case the said one or more functions form the middle layer of the agent, residing between the core and the contracts. In its simplest form a contract can thus include its identifier only.

However, using the approach described above is preferable, since it is much less complicated to define and utilize ready-made views than to generate the views in real time. Furthermore, by means of ready-made views the service level can easily be improved. For example, the system can utilize ready-made views which are taken into use according to the time of day or according to the location of the user.

In order to constrain the maximum number of contracts, a contract can be deleted after it has not been used for a certain time period.

It is also possible to use the system as a "stripped" version so that the same profile information, supplied by the user through the master contract, is available to all clients that are allowed to access the profile information through the contracts.

Anonymous routing can also be utilized for preventing malicious parties from exposing the user agent by correlating the contracts. In this embodiment a different address is attached to each contract of a user agent through the anonymizing network to which the hostels are connected. Since anonymous routing is known as such, it is not discussed in more detail here.

Although the invention was described above with reference to the examples shown in the appended drawings, it is obvious that the invention is not limited to these, but it may be modified by those skilled in the art without departing from the scope and spirit of the invention.

Claims

1. A method for providing user-specific information for the use of service applications in a communications network, the method comprising the steps of

- storing user profile data in user-specific software agents, each agent comprising at least an inner layer for storing the user profile data and an outer layer for storing contracts which form interfaces for controlling the use of the user profile data from the network, the profile data being accessible through the contracts,

- storing said agents in the network,

- making contracts for the use of clients and storing said contracts on the outer layer, each client being an entity utilizing the user profile data in the network,

- maintaining current locations of the contracts in a location information system,

- requesting the location of a desired contract from said system, and

- transferring user-specific information between the client and the agent through said contract.

2. A method according to claim 1, further comprising the step of determining views of the profile data and associating each view with at least one contract, the view defining the form and content of the user-specific information available to the client through the contract with which the view is associated.

3. A method according to claim 2, wherein the step of making contracts includes making a separate master contract for the use of the user only, and at least one service contract for the use of a service application residing in the network.

4. A method according to claim 2, wherein said transferring step includes transferring user-specific information from said location to the client; whereby said information conforms to a view associated with said contract.

5. A method according to claim 3, wherein said transferring step includes transferring user-specific information from the user to said location.

6. A method according to claim 5, wherein user-specific information is supplied by the user to the inner layer through the master contract.

7. A method according to claim 3, wherein making a service contract is initiated by the user.

8. A method according to claim 4, further including the step of storing

the views of the profile data in the agent.

9. A method according to claim 8, wherein the step of transferring user-specific information includes using a view previously stored in the agent.

10. A method according to claim 1, further comprising the step of transferring the agents in the network in response to a change in the location of the user.

11. A method according to claim 1, wherein the step of transferring user-specific information includes encryption of the information.

12. A method according to claim 3, wherein the step of requesting the location is performed at least once for each service session between the user and the client.

13. A method according to claim 1, wherein in client is a service application.

14. A method according to claim 1, wherein the client is the user.

15. A system for providing user-specific information for the use of the service applications in a communications network, the system comprising

- user-specific software agents for storing user profile data, each software agent comprising at least an inner layer for storing said profile data and an outer layer for storing contracts through which the profile data can be accessed by clients, each contract forming an interface for controlling the use of the user profile data from the network and each client being an entity utilizing user profile data in the network,

- storage means for storing said agents in the network,

- location management means for maintaining the current locations of the contracts, and

- means for transferring user-specific information through said contract between the current location of a desired contract and a client.

16. A system according to claim 13, further comprising means for determining views of the profile data and associating each view with at least one contract, each view specifying the form and content of the user-specific information available through the contract with which the view is associated.

17. A system according to claim 14, wherein the user-specific software agents further comprise a middle layer for storing the views, said middle layer being between the outer and inner layers.

18. A system according to claim 13, wherein the user-specific software agents are mobile agents.

19. A system according to claim 13, further comprising agent genera-

tion means for creating a user profile agent.

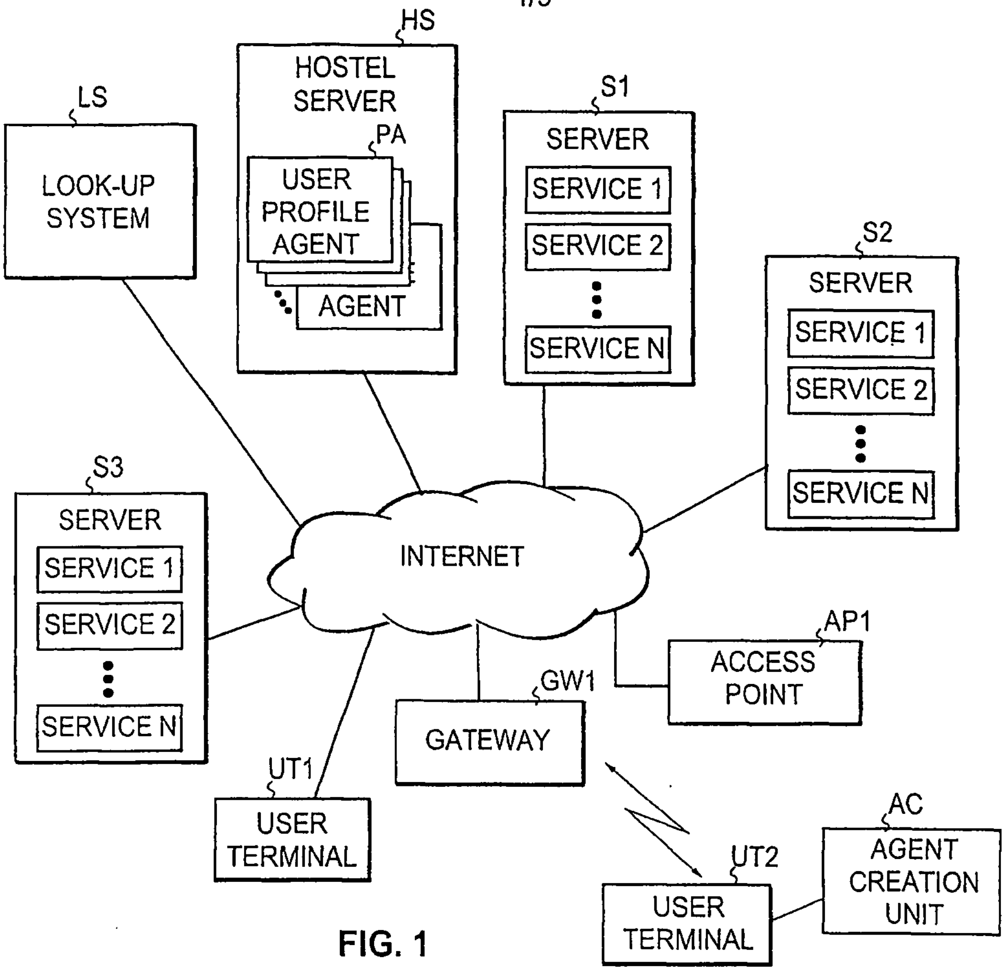

HS
HOSTEL SERVER
PA
USER PROFILE AGENT
AGENT
LS
LOOK-UP SYSTEM
S1
SERVER
SERVICE 1
SERVICE 2
SERVICE N
S2
SERVER
SERVICE 1
SERVICE 2
SERVICE N
S3
SERVER
SERVICE 1
SERVICE 2
SERVICE N
INTERNET
AP1
ACCESS POINT
GW1
GATEWAY
UT1
USER TERMINAL
UT2
USER TERMINAL
AC
AGENT CREATION UNIT

FIG. 1

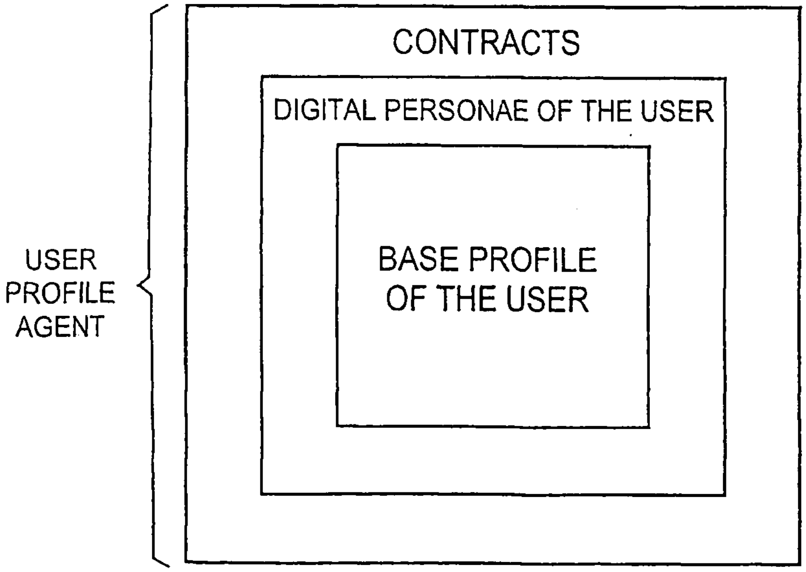

CONTRACTS
DIGITAL PERSONAE OF THE USER
BASE PROFILE OF THE USER
USER PROFILE AGENT

FIG. 2

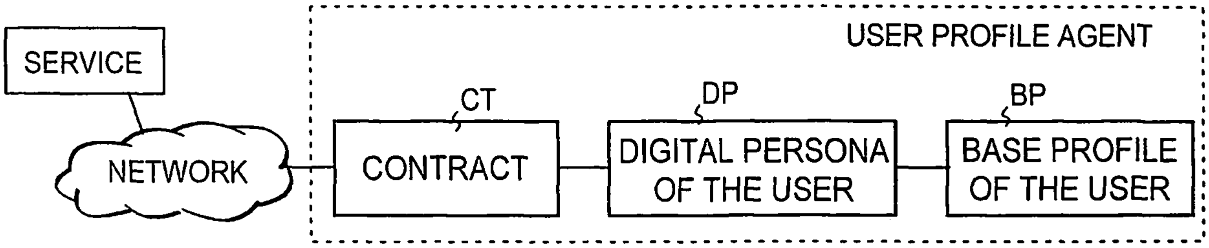


FIG. 3

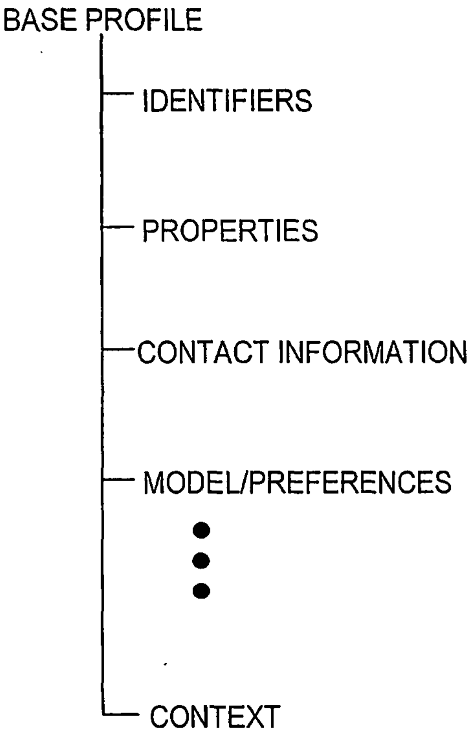


FIG. 4a

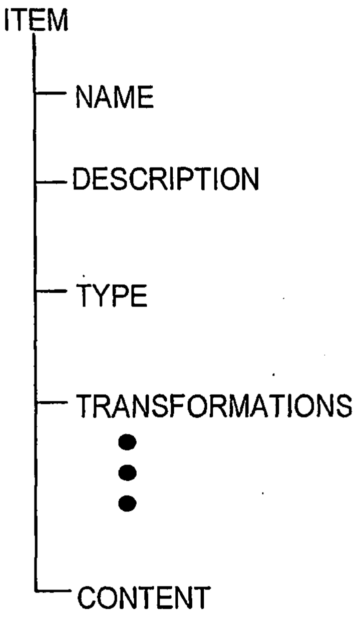


FIG. 4b

- IDENTIFIERS
  - NAME
    - FIRST JOE
    - MIDDLE BAR
    - LAST DOE
    - NICKNAME FOOBAR
- CONTACT INFORMATION
  - ADDRESS
    - POSTAL
      - CATEGORY HOME
      - NAME
        - FIRST JOE
        - LAST DOE
      - STREET 3 ASCOT DRIVE
      - CITY HEREVILLE
      - POSTAL CODE 12345
      - COUNTRY USA
    - POSTAL
      - CATEGORY BUSINESS
      - NAME

        •
        •
        •
- PROPERTIES
  - WEIGHT
    - DESCRIPTION WEIGHT IN KILOGRAMS
    - TYPE POSITIVE FLOAT
    - TRANSFORMATION NUMERIC ABSTRACTION
    - CONTENT 73
  - GENDER
    - TRANSFORMATION SWITCH BETWEEN M, F, AND N
    - CONTENT M
  - INCOME
    - TYPE FLOAT, EUROS
    - CONTENT 50.000
- MODEL/PREFERENCES
  - COM/COMPANY1
    - DESCRIPTION PREFERENCES OF THE SERVICES AT WWW.COMPANY1.COM
    - TYPE FLOAT BETWEEN 0 AND 1
    - SPORTS 0.05
    - BUSINESS 0.25
    - WEATHER 0.15

      •
      •
      •
- CONTEXT
  - CURRENT/GEO
    - DESCRIPTION USER'S COORDINATES
    - TYPE COORDINATE
    - TRANSFORMATION NUMERIC ABSTRACTION
    - CONTENT 60.302 N, 24.561 E

BASE PROFILE OF THE USER

FIG. 5

BUSINESS PERSONA

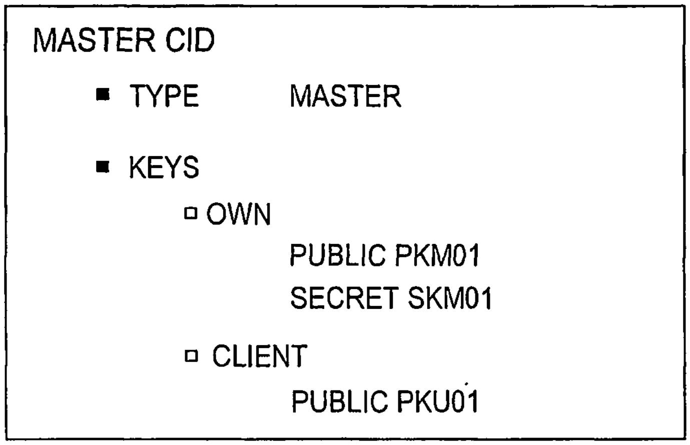
- TRANSFORMATIONS
    - MODEL/PREFERENCES /COM/COMPANY1
        - MULTIPLY "BUSINESS" BY 3, ADJUST OTHERS UNIFORMLY
- MASKS
    - IDENTIFIERS/NAME/NICKNAME
        - HIDE

FIG. 6

ONLINE PERSONA

- TRANSFORMATIONS
    - PROPERTIES/GENDER
        - SWITCH TO N
    - PROPERTIES/INCOME
        - ROUND TO NEAREST 10000
- MASKS
    - IDENTIFIERS/NAME/
        - HIDE EXCEPT "NICKNAME"
    - CONTACT INFORMATION/ADDRESS/POSTAL
        - WHERE CATEGORY=HOME
          HIDE

FIG. 7

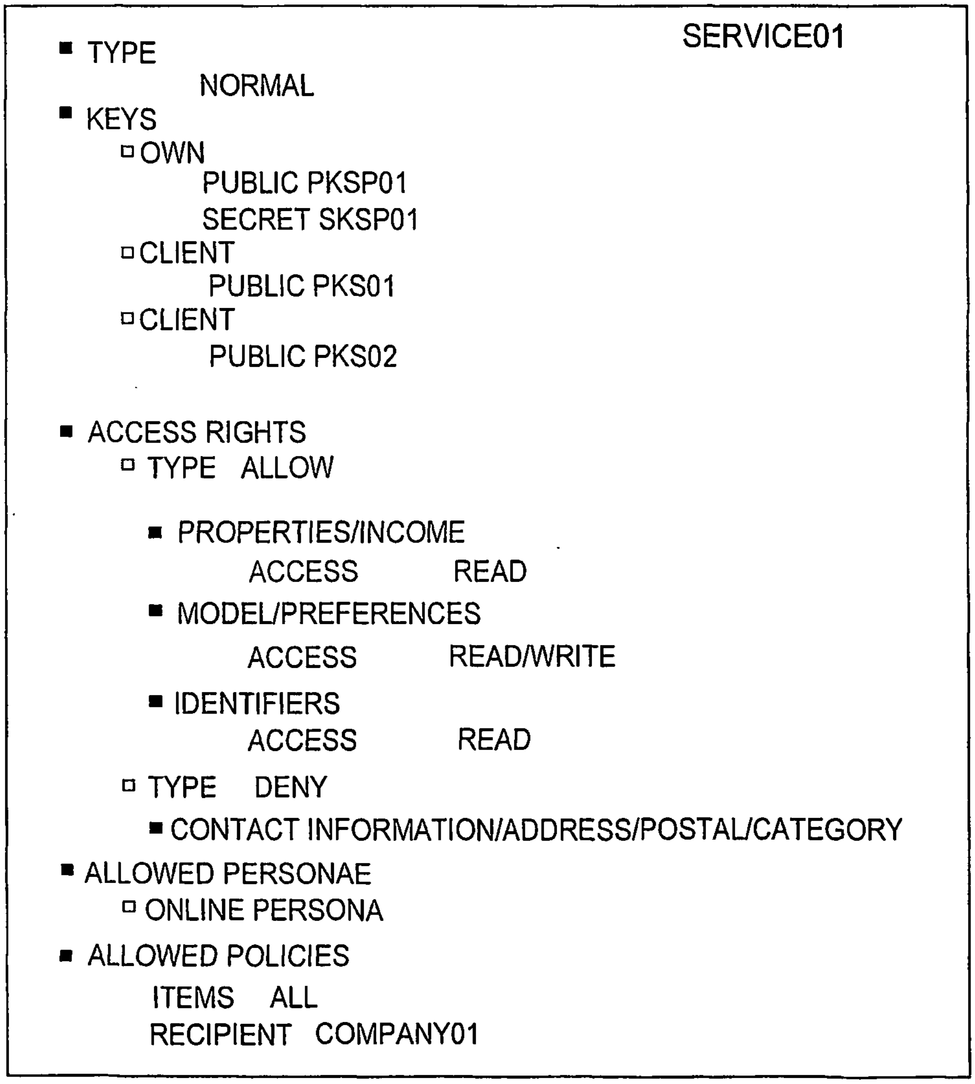


```
MASTER CID
    ■ TYPE        MASTER

    ■ KEYS
          □ OWN
                PUBLIC PKM01
                SECRET SKM01

          □ CLIENT
                PUBLIC PKU01
```

FIG. 8



```
                                          SERVICE01
  ■ TYPE
          NORMAL
  ■ KEYS
      □ OWN
          PUBLIC PKSP01
          SECRET SKSP01
      □ CLIENT
          PUBLIC PKS01
      □ CLIENT
          PUBLIC PKS02

  ■ ACCESS RIGHTS
      □ TYPE   ALLOW

        ■ PROPERTIES/INCOME
              ACCESS        READ
        ■ MODEL/PREFERENCES
              ACCESS        READ/WRITE
        ■ IDENTIFIERS
              ACCESS        READ
      □ TYPE   DENY
        ■ CONTACT INFORMATION/ADDRESS/POSTAL/CATEGORY
  ■ ALLOWED PERSONAE
      □ ONLINE PERSONA
  ■ ALLOWED POLICIES
        ITEMS    ALL
        RECIPIENT   COMPANY01
```

FIG. 9

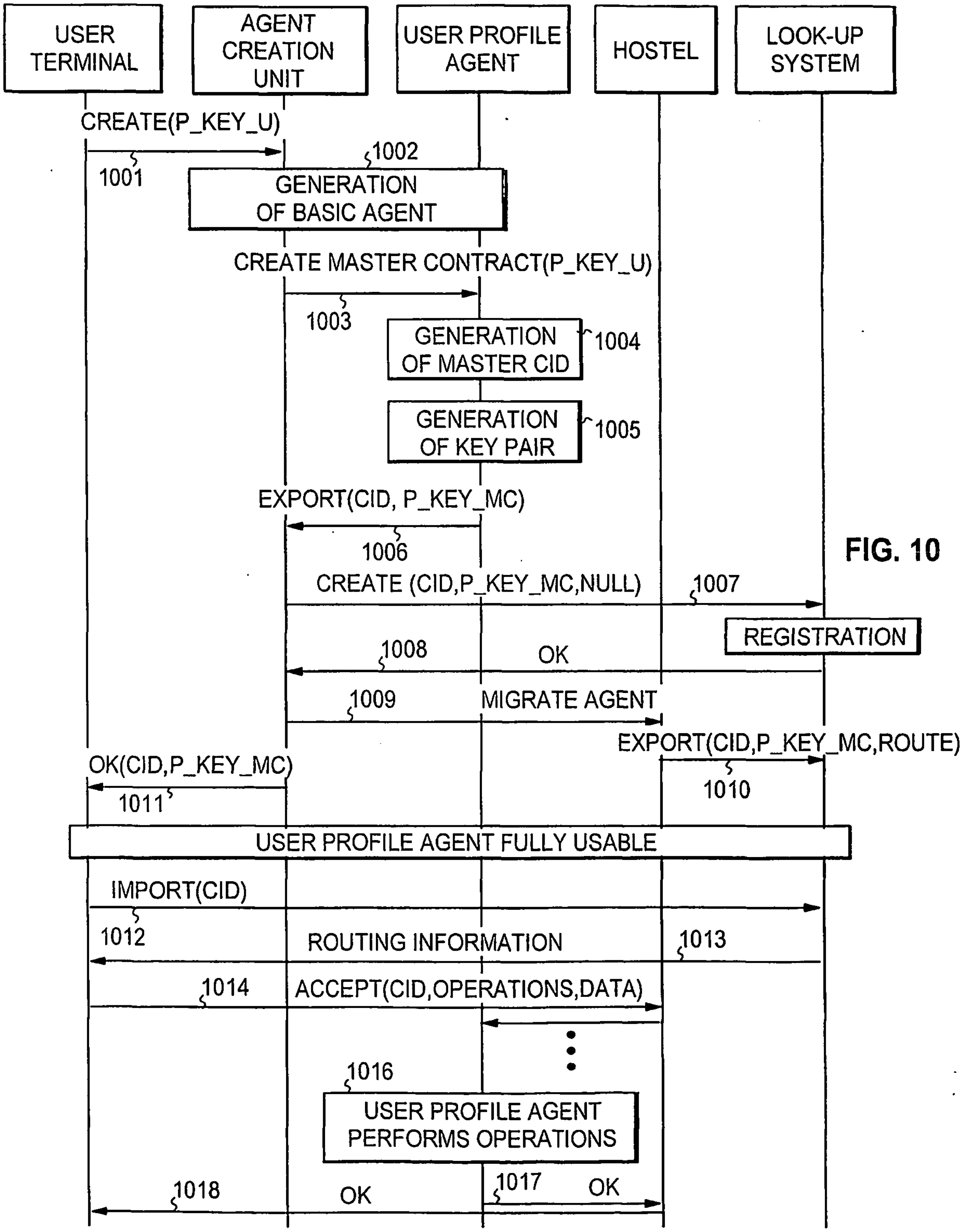

USER TERMINAL
AGENT CREATION UNIT
USER PROFILE AGENT
HOSTEL
LOOK-UP SYSTEM
CREATE(P_KEY_U)
1001
1002
GENERATION OF BASIC AGENT
CREATE MASTER CONTRACT(P_KEY_U)
1003
GENERATION OF MASTER CID
1004
GENERATION OF KEY PAIR
1005
EXPORT(CID, P_KEY_MC)
1006
CREATE (CID,P_KEY_MC,NULL)
1007
REGISTRATION
1008
OK
1009
MIGRATE AGENT
EXPORT(CID,P_KEY_MC,ROUTE)
1010
OK(CID,P_KEY_MC)
1011
USER PROFILE AGENT FULLY USABLE
IMPORT(CID)
1012
ROUTING INFORMATION
1013
1014
ACCEPT(CID,OPERATIONS,DATA)
1016
USER PROFILE AGENT PERFORMS OPERATIONS
1017
OK
1018
OK

FIG. 10

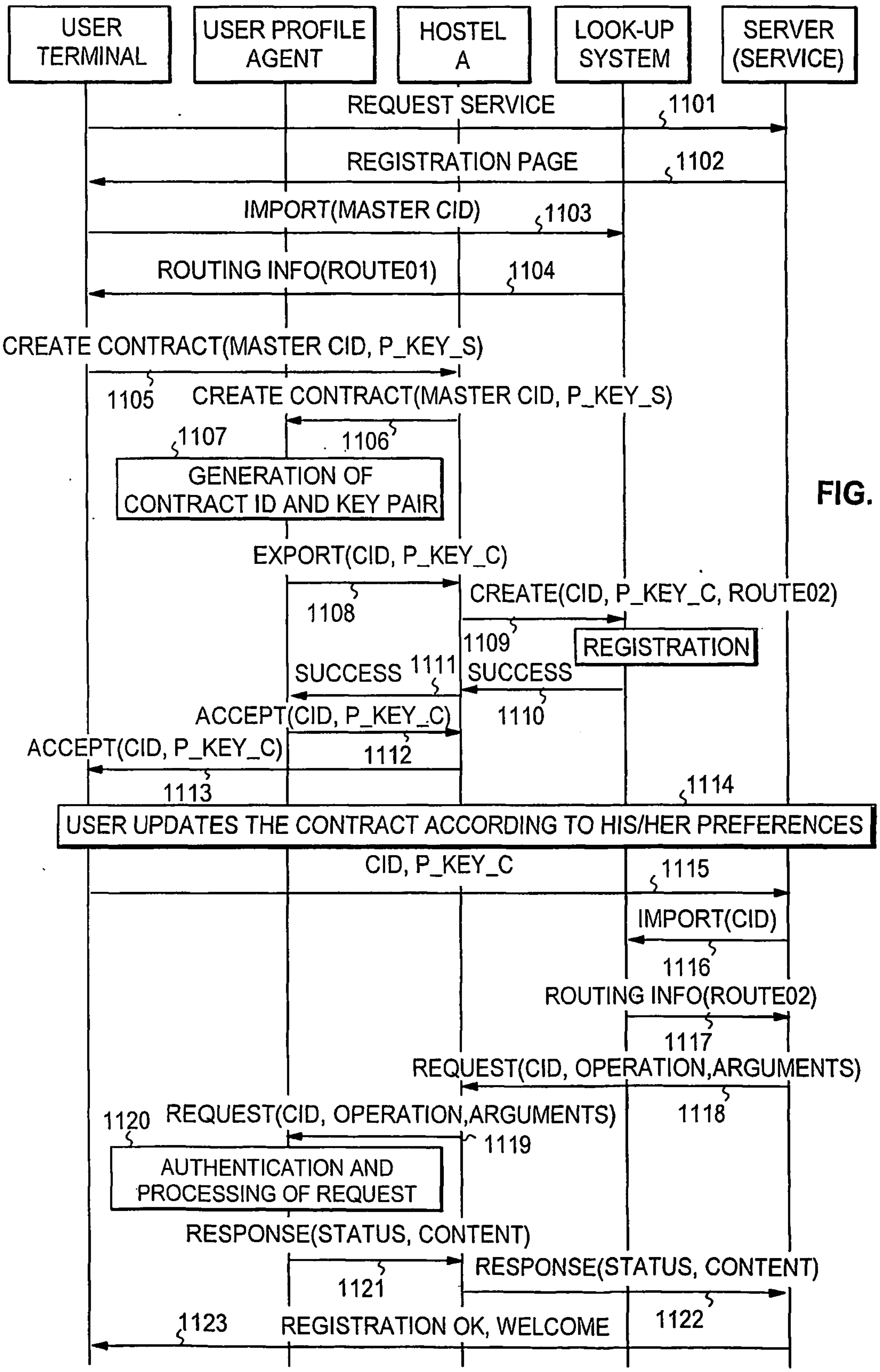

USER TERMINAL
USER PROFILE AGENT
HOSTEL A
LOOK-UP SYSTEM
SERVER (SERVICE)
REQUEST SERVICE
1101
REGISTRATION PAGE
1102
IMPORT(MASTER CID)
1103
ROUTING INFO(ROUTE01)
1104
CREATE CONTRACT(MASTER CID, P_KEY_S)
1105
CREATE CONTRACT(MASTER CID, P_KEY_S)
1106
1107
GENERATION OF CONTRACT ID AND KEY PAIR
EXPORT(CID, P_KEY_C)
1108
CREATE(CID, P_KEY_C, ROUTE02)
1109
REGISTRATION
SUCCESS
1111
SUCCESS
1110
ACCEPT(CID, P_KEY_C)
1112
ACCEPT(CID, P_KEY_C)
1113
1114
USER UPDATES THE CONTRACT ACCORDING TO HIS/HER PREFERENCES
CID, P_KEY_C
1115
IMPORT(CID)
1116
ROUTING INFO(ROUTE02)
1117
REQUEST(CID, OPERATION,ARGUMENTS)
1118
1120
REQUEST(CID, OPERATION,ARGUMENTS)
1119
AUTHENTICATION AND PROCESSING OF REQUEST
RESPONSE(STATUS, CONTENT)
1121
RESPONSE(STATUS, CONTENT)
1122
1123
REGISTRATION OK, WELCOME

FIG. 11

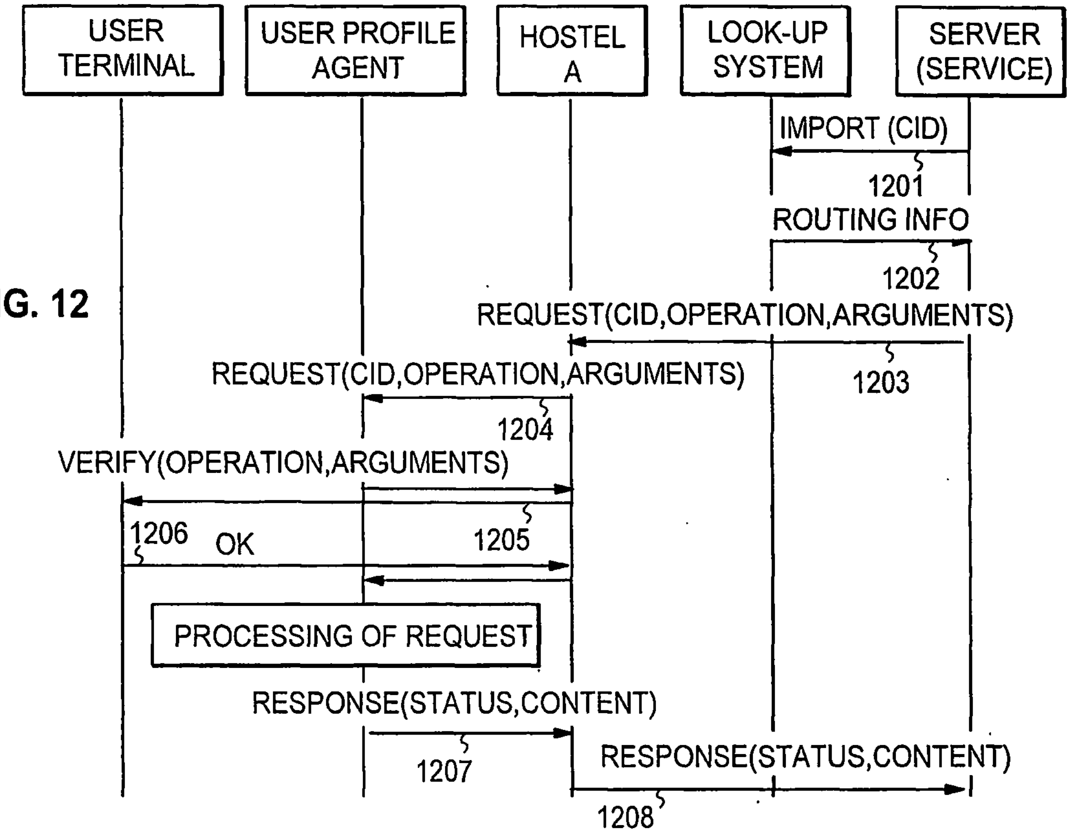

USER TERMINAL
USER PROFILE AGENT
HOSTEL A
LOOK-UP SYSTEM
SERVER (SERVICE)
IMPORT (CID)
1201
ROUTING INFO
1202
REQUEST(CID,OPERATION,ARGUMENTS)
1203
REQUEST(CID,OPERATION,ARGUMENTS)
1204
VERIFY(OPERATION,ARGUMENTS)
1205
1206
OK
PROCESSING OF REQUEST
RESPONSE(STATUS,CONTENT)
1207
RESPONSE(STATUS,CONTENT)
1208

FIG. 12

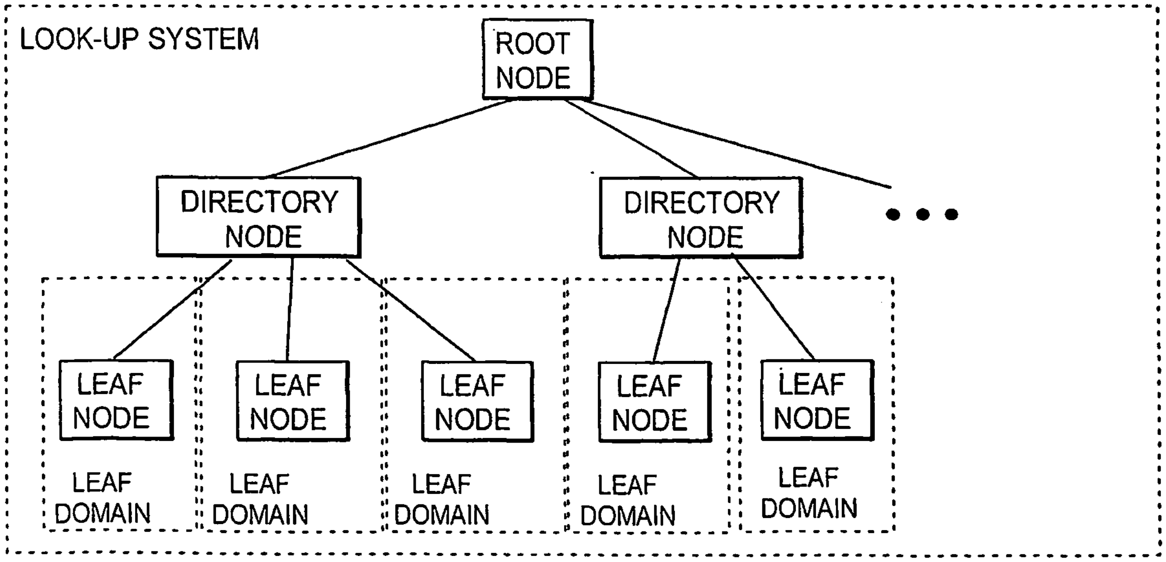
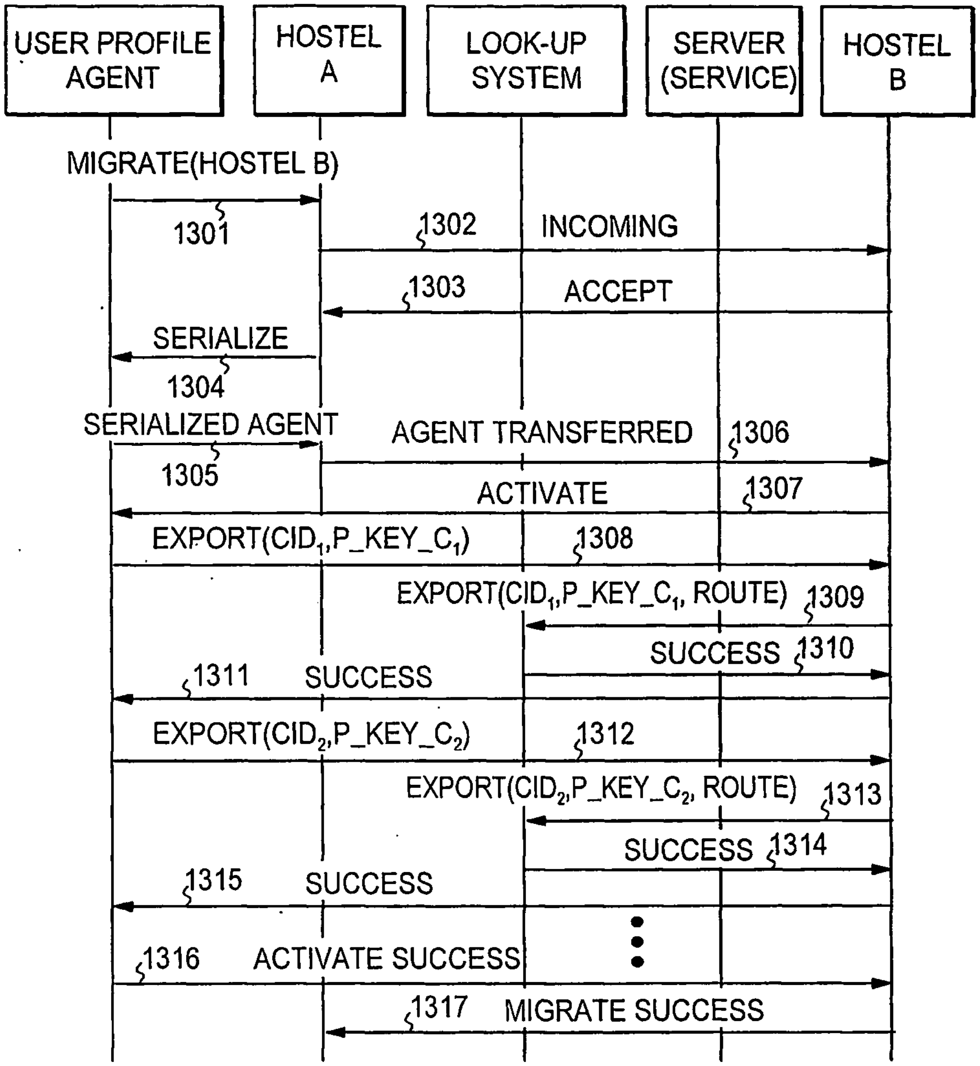

LOOK-UP SYSTEM
ROOT NODE
DIRECTORY NODE
DIRECTORY NODE
LEAF NODE
LEAF NODE
LEAF NODE
LEAF NODE
LEAF NODE
LEAF DOMAIN
LEAF DOMAIN
LEAF DOMAIN
LEAF DOMAIN
LEAF DOMAIN

FIG. 14

FIG. 13


USER PROFILE AGENT
HOSTEL A
LOOK-UP SYSTEM
SERVER (SERVICE)
HOSTEL B
MIGRATE(HOSTEL B)
1301
1302
INCOMING
1303
ACCEPT
SERIALIZE
1304
SERIALIZED AGENT
1305
AGENT TRANSFERRED
1306
ACTIVATE
1307
EXPORT(CID$_1$,P_KEY_C$_1$)
1308
EXPORT(CID$_1$,P_KEY_C$_1$, ROUTE)
1309
SUCCESS
1310
1311
SUCCESS
EXPORT(CID$_2$,P_KEY_C$_2$)
1312
EXPORT(CID$_2$,P_KEY_C$_2$, ROUTE)
1313
SUCCESS
1314
1315
SUCCESS
1316
ACTIVATE SUCCESS
1317
MIGRATE SUCCESS

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 01/00430

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 17/30, G06F 17/60
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0953920 A2 (BRITISH TELECOMMUNICATIONS), 3 November 1999 (03.11.99), column 4, line 8 - column 5, line 26, figure 1, abstract --	1-19
X	GB 2335761 A (MITEL CORPORATION), 29 Sept 1999 (29.09.99), page 4, line 13 - page 5, line 30, figure 1, abstract --	1-19
X	GB 2328110 A (MITEL CORPORATION), 10 February 1999 (10.02.99), page 3, line 21 - page 5, line 31, figure 2, abstract -- --------	1-19

□ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 24 August 2001	Date of mailing of the international search report 27 -08- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Oskar Pihlgren/LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/08/01

International application No.

PCT/FI 01/00430

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0953920 A2	03/11/99	EP 0807291 A,B	19/11/97
		AU 707050 B	01/07/99
		AU 4454996 A	14/08/96
		BR 9606931 A	11/11/97
		CA 2210581 A	01/08/96
		CN 1169195 A	31/12/97
		DE 69606021 D,T	03/08/00
		FI 973080 A	22/07/97
		HK 1004832 A	00/00/00
		JP 10513587 T	22/12/98
		NO 973372 A	22/09/97
		NZ 298861 A	28/01/99
		WO 9623265 A	01/08/96
GB 2335761 A	29/09/99	DE 19913509 A	30/09/99
		GB 9806392 D	00/00/00
GB 2328110 A	10/02/99	GB 9716393 D	00/00/00